



Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 68/2026 du 9 avril 2026

Objet : avis relatif à un avant-projet de loi complétant les lois sur le Conseil d'État, coordonnées le 12 janvier 1973, par des dispositions relatives aux lanceurs d'alerte (CO-A-2026-008)

Mots-clés : délai de conservation maximal – responsable conjoint du traitement – documents administratifs – Conseil d'État lanceurs d'alerte – canal de signalement interne

Traduction

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après le "RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis de Madame Annelies Verlinden, Ministre de la Justice (ci-après : le "demandeur"), reçue le 13 janvier 2026 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après "l'Autorité") émet l'avis suivant le 9 avril 2026 :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le 13 janvier 2026, le demandeur a sollicité l'avis de l'Autorité concernant un avant-projet de loi *complétant les lois sur le Conseil d'État, coordonnées le 12 janvier 1973, par des dispositions relatives aux lanceurs d'alerte* (ci-après : le Projet).
2. Le Projet porte sur la transposition partielle de la Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 *sur la protection des personnes qui signalent des violations du droit de l'Union* (ci-après : la Directive) en ce qui concerne les membres du personnel administratif, les personnes visées aux articles 102*bis* et 102*ter* et les titulaires de fonction du Conseil d'État.¹ Cela se traduit par l'ajout d'un nouveau chapitre IX "*Protection des lanceurs d'alerte*" au Titre VII ("*De l'organisation du Conseil d'État*") des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, contenant les articles 115/1 à 115/11.
3. Le présent Projet complète les transpositions précédentes de la Directive, à savoir la loi du 28 novembre 2022 *sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé*, et la loi du 8 décembre 2022 *relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée*.
4. Étant donné que la loi du 8 décembre 2022 ne s'applique pas au personnel de l'ordre judiciaire, un avant-projet de loi intitulé "*Avant-projet de loi relatif aux canaux de signalement et à la protection des auteurs de signalements d'atteintes à l'intégrité au sein des organes du pouvoir judiciaire visés dans la deuxième partie, livre I^{er}, du Code judiciaire, au sein de l'Institut de formation judiciaire et au sein du Conseil consultatif de la magistrature, à l'exception du Conseil supérieur de la Justice*" est en préparation, lequel porte sur les juges, les membres du ministère public, les greffiers, les membres du personnel des greffes et parquets, ainsi que sur les stagiaires et fait également l'objet d'une demande d'avis auprès de l'Autorité.
5. Par dérogation à ce qui précède, le présent Projet s'applique au Conseil d'État en tant que *lex specialis* par rapport à la norme mentionnée au point 4, de sorte que cette norme reste d'application, sauf dans la mesure où le projet prévoit expressément un autre régime.²

¹ Article 115/1 du Projet.

² Commentaire des articles, p. 1.

II. EXAMEN QUANT AU FOND

II.1 Base juridique

6. *Rappel des principes* : Chaque traitement de données à caractère personnel doit avoir une base juridique ou de licéité, comme le prévoit l'article 6, paragraphe 1 du RGPD. Les traitements de données qui sont instaurés par une mesure normative sont presque toujours basés sur l'article 6.1, point c) ou e) du RGPD³. Le lecteur est renvoyé à l'application de ces principes tels que définis ci-après.
7. **En plus de devoir être nécessaire et proportionnée**, toute norme régissant le traitement de données à caractère personnel (et constituant par nature une ingérence dans le droit à la protection des données à caractère personnel) **doit répondre aux exigences de prévisibilité et de précision afin que les personnes concernées au sujet desquelles des données sont traitées aient une idée claire du traitement de leurs données**. En vertu de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la Constitution et 8 de la CEDH, une telle norme doit décrire les éléments essentiels des traitements allant de pair avec l'ingérence de l'autorité publique :
- la (les) finalité(s) précise(s) et concrète(s) des traitements de données ;
 - la désignation du (des) responsable(s) du traitement (à moins que cela ne soit clair).
8. Par ailleurs, conformément au principe de légalité et de prévisibilité, la norme formelle doit également comprendre les éléments essentiels (complémentaires) suivants⁴ :
- les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
 - les catégories de personnes concernées dont les données à caractère personnel seront traitées ;
 - les (catégories de) destinataires des données à caractère personnel ainsi que les circonstances dans lesquelles ils reçoivent les données et les motifs y afférents ;
 - le délai maximal de conservation des données à caractère personnel enregistrées ;
 - l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

³ Article 6, paragraphe 1 du RGPD : "*Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (...)*

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; (...)".

⁴ Voir DEGRAVE, E., "*L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (Voir entre autres : CJUE, l'arrêt *Rotaru c. Roumanie*, 4 mai 2000) ; voir également plusieurs arrêts de la Cour constitutionnelle : l'arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'arrêt n° 29/2018 du 15 mars 2018 (p. 26).

9. *Application concrète* : le traitement de données à caractère personnel auquel le Projet soumis pour avis donne lieu repose sur l'article 6.1.c) du RGPD⁵. Considérant que le Projet implique un traitement de données à caractère personnel *i) qui porte sur des catégories particulières de données à caractère personnel (données sensibles) au sens des articles 9 et/ou 10 du RGPD et/ou sur des données hautement personnelles ; ii) qui concerne des personnes vulnérables ; iii) qui a lieu à des fins de surveillance ou de contrôle ; iv) au cours duquel les données sont communiquées ou accessibles à des tiers ; v) qui peut donner lieu à une décision ayant des conséquences négatives pour les personnes concernées*, l'Autorité estime qu'il est question en l'espèce d'une ingérence importante, ce qui rend d'autant plus importante l'obligation – déjà existante – de définir les éléments essentiels.
10. L'Autorité vérifiera ci-après si et dans quelle mesure l'avant-projet de loi qui est à présent soumis pour avis respecte les principes de protection des données tels qu'ils découlent du RGPD et de la LTD, en particulier.

II.2 Commentaire des articles

11. Après analyse de l'ensemble des documents, l'Autorité constate que le Projet contient des dispositions portant sur divers aspects qui ne sont pas nécessairement liés à la réglementation du traitement des données à caractère personnel. L'Autorité limite donc l'examen qui suit aux dispositions pertinentes à cet égard.

ARTICLE 115/3

12. Le projet d'article 115/3 régit la composition du canal de signalement interne, à savoir quatre membres dont deux issus du Conseil ou du Bureau de coordination et deux de l'Auditorat, la parité linguistique étant garantie par la présence de deux membres néerlandophones et de deux membres francophones. D'autres conditions sont également fixées, notamment les conditions de nomination, certains motifs d'exclusion, un avis préalable, une durée de mandat renouvelable de 6 ans et la désignation de membres suppléants.

ARTICLE 115/4

13. Le projet d'article 115/4 prévoit la possibilité pour l'auteur de signalement de choisir la personne chargée du suivi et du retour d'information relatifs à son signalement. À défaut d'un tel choix, les membres du canal de signalement interne en décident entre eux.

⁵ Article 6.1.e) du RGPD : *"le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement."*

ARTICLE 115/5

14. Le projet d'article 115/5 dispose que le canal de signalement interne, voir infra, est désigné comme responsable du traitement pour les données à caractère personnel traitées dans le cadre des signalements internes qu'il reçoit. L'Autorité en prend acte, mais souligne néanmoins que des situations de responsabilité conjointe du traitement pourront également se présenter, par exemple lors de la transmission de signalements au Comité visé à l'article 6, 3^o de la norme mentionnée au point 4.

ARTICLE 115/6

15. Le projet d'article 115/6, qui transpose l'article 16 de la Directive, fait du devoir de confidentialité une mesure *ex ante* essentielle pour prévenir les représailles. Une telle mesure est également justifiée au regard du droit au respect de la vie privée et du droit à la protection des données. La confidentialité de l'identité ne concerne pas seulement celle de l'auteur de signalement, mais aussi celle des tiers pouvant être associés à celui-ci, du facilitateur et des personnes ayant coopéré à l'enquête.⁶
16. L'identité de l'auteur de signalement et celle des autres personnes concernées ne peuvent en aucun cas être divulguées⁷ sans leur consentement exprès et libre à d'autres personnes que les membres du personnel habilités pour la réception ou le suivi de signalements. Cela s'applique également pour toute autre information à partir de laquelle l'identité de l'auteur de signalement ou des autres personnes concernées peut être directement ou indirectement déduite. Le commentaire des articles ajoute qu'en sa qualité de responsable du traitement, le canal de signalement interne est tenu de prendre des mesures techniques et organisationnelles appropriées afin de garantir une protection adéquate des données à caractère personnel ; il est notamment fait référence à une politique stricte de contrôle des accès avec une limitation des personnes pouvant accéder aux données, une utilisation d'une authentification fiable et une journalisation des accès.⁸
17. En ce qui concerne l'utilisation d'une authentification fiable, il est recommandé d'opter pour une connexion basée sur l'eIDAS, au minimum de niveau "substantiel" et de préférence de niveau "élevé". Dans la pratique, cela revient à utiliser le CSAM/FAS du BOSA pour la connexion (avec eID, l'application MyGov.be ou Itsme). En outre, d'autres mesures techniques et organisationnelles doivent être envisagées, telles que la pseudonymisation ou l'anonymisation des signalements lorsque cela est possible, le chiffrement des données, tant lors du stockage que lors de la transmission, le stockage séparé des données d'identité et du contenu des signalements, des délais de conservation clairs et une suppression automatique des données, des audits de sécurité réguliers et des tests des systèmes de signalement, une formation et des obligations de confidentialité pour les membres du personnel chargés du traitement des signalements, ainsi que des procédures de réponse aux incidents en cas de

⁶ Article 115/6, Commentaire des articles, p. 3.

⁷ Article 4(11) du RGPD.

⁸ Article 115/6, Commentaire des articles, p. 3.

fuites de données. Enfin, en ce qui concerne le suivi de la sécurité, il convient de veiller en temps utile à la résolution des problèmes de sécurité logicielle, en accordant une attention particulière aux éventuels problèmes de sécurité connus signalés par les fabricants/développeurs et le Centre pour la cybersécurité Belgique (CCB)⁹.

18. Le Projet prévoit toutefois que, dans la mesure du possible, une version anonymisée du document administratif puisse être fournie, et ce uniquement lorsque le contexte ne permet en aucun cas de déduire des données à caractère personnel ou des données relatives à l'identité. **Le demandeur est prié de fournir des précisions supplémentaires sur la raison de l'introduction de cette possibilité. Il convient en particulier de préciser s'il s'agit de protéger les droits de la défense, qui sont déjà garantis par le deuxième paragraphe du projet d'article 115/6, ou s'il s'agit de transparence dans le cadre de la publicité de l'administration.** Bien que l'introduction d'une telle mesure contribue à un degré plus élevé de transparence, le demandeur doit tenir compte du risque de réidentification. Il est en effet possible que le simple exposé du contexte ou des faits d'atteinte à l'intégrité permette déjà de déduire l'identité de l'auteur de signalement, par exemple sur la base d'éléments tels que la relation hiérarchique, le lieu, etc.
19. Par dérogation toutefois à ce qui précède, l'identité de l'auteur de signalement (et des tiers) ainsi que toute autre information permettant de déduire l'identité de ces personnes "*peuvent être divulguées uniquement lorsqu'il s'agit d'une obligation nécessaire et proportionnée imposée par une législation spéciale dans le cadre d'enquêtes menées par des autorités nationales ou dans le cadre de procédures judiciaires, notamment en vue de sauvegarder les droits de la défense de la personne concernée.*" Dans ce cas, les personnes concernées en sont informées, à moins qu'une telle information ne risque de compromettre les enquêtes ou les procédures judiciaires concernées. L'Autorité estime que l'exigence de disposer d'une obligation **explicite, nécessaire et proportionnée** en vertu du droit de l'Union ou du droit national offre suffisamment de garanties en ce qui concerne la protection des données à caractère personnel. Une telle norme implique en effet *de facto* la présence d'une finalité légitime pour la divulgation de l'identité de l'auteur de signalement ou des personnes concernées. Il n'empêche bien entendu que toute norme qui crée un motif d'exception (et engendre ainsi une ingérence importante dans les droits et libertés des personnes concernées), conformément à l'article 36, paragraphe 4 du RGPD, lu conjointement avec l'article 57, paragraphe 1, c) et le considérant 96 de ce même règlement, doit avant tout être soumise à l'avis de l'Autorité.
20. L'Autorité constate par ailleurs que le Projet indique que "*En particulier, le traitement ultérieur des données doit être conforme à l'article 6.1, c) et e), du règlement (UE) 2016/679.*" Il va de soi que les données doivent être traitées lorsqu'il est nécessaire de respecter une obligation légale à laquelle le

⁹ Voir à cet égard : CCB, *Cyber Threat Research & Intelligence Sharing*, consulté la dernière fois le 26 mars 2026, à l'adresse <<https://ccb.belgium.be/fr/cytris>>; CCB, *Administration*, consulté la dernière fois le 26 mars 2026, à l'adresse <<https://ccb.belgium.be/fr/administration>>.

responsable du traitement est soumis ou lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. On ne sait toutefois pas clairement ce que l'on vise exactement dans ce contexte en prévoyant cette précision expresse.

ARTICLE 115/7

21. Le projet d'article 115/7 définit les finalités concrètes et précises du traitement des données à caractère personnel dans le cadre des signalements internes et des divulgations, à savoir vérifier l'exactitude des allégations contenues dans le signalement ou la divulgation et, si nécessaire, traiter l'atteinte à l'intégrité signalée. L'Autorité en prend acte.

ARTICLE 115/8

22. Le projet d'article 115/8, qui est une transposition de l'article 18 de la Directive, concerne l'enregistrement des signalements. Il prévoit que les entités juridiques des secteurs privé et public ainsi que les autorités compétentes doivent tenir un registre de chaque signalement reçu.
23. La disposition énonce trois hypothèses spécifiques en fonction de la forme du signalement, à savoir un signalement oral avec enregistrement de la conversation, un signalement oral sans enregistrement de la conversation ou un compte rendu précis de la conversation.
24. Le demandeur doit s'assurer qu'il est également clair pour l'auteur de signalement que le fait d'effectuer le signalement équivaut à donner son consentement au traitement de toutes les données qu'il fournit. À cet égard, il est rappelé au demandeur qu'il appartient au responsable du traitement, compte tenu de sa responsabilité, de démontrer qu'aucune donnée n'a été traitée au-delà de ce qui est nécessaire.
25. À cet égard, l'Autorité constate que la disposition en question fait mention d'enregistrement et d'archive. Il est rappelé au demandeur que l'enregistrement des signalements (qui constitue un traitement) n'est licite qu'au regard des finalités prévues (voir point 21). Ceci est étayé dans le commentaire des articles par l'argument selon lequel "*L'implémentation d'un mécanisme de signalement implique un exercice d'équilibre pour tenir compte des intérêts de tous les protagonistes (l'organisation, l'auteur de signalement et la personne concernée). L'intérêt de l'organisation se reflète dans des règles d'archivage internes portant la préservation et la conservation des documents administratifs.*"
26. Toutefois, l'on ne sait toujours pas clairement quel est le but de l'archivage et quelles données seront conservées : enregistre-t-on uniquement le signalement initial, ou également le déroulement entier du suivi ; l'archivage sert-il uniquement de 'lieu de stockage' pour les signalements ou s'agit-il pour ainsi dire de la plateforme centrale au sein des canaux de signalement interne et externe pour le traitement des signalements ; quelles personnes ont accès au contenu de l'archivage ; sous quelles conditions

peut-il y avoir un transfert de données entre les archivages des autorités compétentes ? ... Ces éléments doivent être précisés dans le Projet. Sur cette base, on pourra définir par la suite des directives ou modalités de fonctionnement supplémentaires.

27. Enfin, le 5^e paragraphe dispose que "*Tous les documents pertinents relatifs à une enquête dans le cadre d'un signalement via un canal de signalement interne sont conservés pendant dix ans.*"
28. L'attention du demandeur est attirée à cet égard sur le fait qu'en vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Cela signifie que, si la finalité est atteinte avant l'expiration du délai de conservation prévu de 10 ans, ces données doivent être supprimées. Toutefois, pour pouvoir déterminer à quel moment ce délai de conservation prend effet, il convient de prévoir une date de début. Ainsi, le délai de conservation peut prendre effet au moment de la réception du signalement, mais il peut également recommencer à courir à chaque nouvelle étape de la procédure, telle que la rédaction de rapports écrits ou la clôture du rapport d'enquête.
29. En outre, il est essentiel de renvoyer le demandeur à la jurisprudence du Conseil d'État, qui fait référence à un délai de conservation maximal et non à un délai de conservation général fixe.¹⁰ Ainsi, un même délai de conservation ne peut en aucun cas s'appliquer aux signalements ayant donné lieu à une enquête et à ceux qui sont restés sans suite. Il est donc demandé de modifier le Projet en supprimant le terme "pendant" et en le remplaçant par la notion de "au maximum", tout en tenant compte des différents scénarios qui nécessitent des délais de conservation différents.

ARTICLE 115/9

30. Le projet d'article 115/9 fait référence au Comité visé à l'article 14 de l'avant-projet de loi mentionné au point 4, qui confie la mission du canal de signalement externe à un organe indépendant, dénommé le Comité, composé d'un magistrat de la Cour constitutionnelle, d'un magistrat de la Cour de cassation et d'un magistrat du Conseil d'État. Cette disposition régit en outre la procédure et la composition du canal de signalement externe, ainsi que le cadre concernant le membre et le membre suppléant de la Cour au sein du Comité. Cette disposition n'appelle pas d'autre remarque.

¹⁰ AV. CDE 68.936/AG du 7 avril 2021 sur un avant-projet de loi ayant donné lieu à la loi du 14 août 2021 *relative aux mesures de police administrative lors d'une situation d'urgence épidémique*, Doc. Parl. Chambre, 2020-21, n° 55-1951/001, 119.

PAR CES MOTIFS,

l'Autorité estime que :

1. La désignation du responsable du traitement doit être complétée de manière à mentionner les cas de responsabilité conjointe du traitement (**point 13**) ;
2. Il est recommandé au demandeur de tenir compte des mesures techniques et organisationnelles proposées (**point 17**) ;
3. Le demandeur doit préciser davantage la raison et les conditions d'application de la version anonymisée des documents administratifs, en accordant une attention particulière au risque de réidentification (**point 18**) ;
4. Le demandeur doit préciser la portée de la possibilité de traitement ultérieur, telle que visée par la référence à l'article 6, paragraphe 1, points c) et e) du RGPD (**point 20**) ;
5. Le demandeur doit garantir que l'auteur de signalement est clairement informé du traitement des données fournies et que seules les données nécessaires à la finalité sont traitées (**point 24**) ;
6. Il convient d'apporter des précisions concernant l'archive et l'enregistrement (**points 22-26**) ;
7. Il convient de prévoir un délai de conservation maximal dans le Projet (**points** Error! Reference source not found.-Error! Reference source not found.).

Pour le Service d'Autorisation et d'Avis,
(sé) Alexandra Jaspar, Directrice